Description

BACKGROUND OF THE INVENTION

Automatic Teller Machines (A.T.M.s) have been a revolutionary invention that offers bank customers twenty-four hour access to their deposits. However, these machines have opened the opportunity for lucrative thieves to wait for the right opportunity to coerce vulnerable customers to withdraw large sums of cash. Since these thieves are often not caught on videotape (some are wise enough to stand away from area under surveillance), customers are at risk of having substantial cash stolen. These customers are particularly vulnerable once they are confronted by their attacker since all means of contacting authorities (via cell phone, for instance) are curtailed by the attacker's watchful eye on the victim's actions.

Thus, because bank users are not able to contact public or private authorities during the commission of a crime, they are in danger of having substantial cash stolen and/or having substantial bodily injury imposed without the security of a patrol car on the way.

There have been several attempts to confront this pressing problem. Colbert (U.S. Pat. No. 5,594,806) attempts to fix this by having the computer camera focus on the knuckles of a user and thus allows for a form of identification of bank customers. While this may be useful for accurately identifying the bank user, it provides no security to bank users who are coerced by criminals to withdraw substantial cash that will be stolen after the

bank transaction. Kroll (U.S. Pat. No. 6,062,474) also addresses this security lapse by proposing that A.T.Ms memorize the speed and nuances of each bank customer typing their P.I.N. and only accepting transactions that fit similar A.T.M. key-punched P.I.N. patterns of the respective bank customer. While this may successfully block unauthorized individuals from completing a transaction with a victim's ATM card, this does not empower each bank customer to individually contact security under dangerous circumstances.

A better method of A.T.M. security is by empowering each bank customer to take charge of their own safety by enabling them to create a second P.I.N. that will serve to be used exclusively to send the hidden message that emergency police protection is needed. This method relies on the ingenuity and accuracy of the bank customer to make the individual decision to contact security through their emergency P.I.N. rather than placing trust in the A.T.M. machine to detect suspicious activity, which is one of the weaknesses of Kroll's ATM security upgrade (U.S. Pat. No.6,062,474). When customer uses their emergency P.I.N. there should not be any visual or audible confirmation of such a request. The A.T.M. should withdraw the amount requested by the customer to minimize potential confrontations between him/her and the criminal.

Inventor: Michael Scott Gordon

Citizen: United States of America

4807 Ambrose Ave,

Los Angeles, CA 90027

References:

6,062,474	**October 2, 1997**	**235/382**
6,073,106	**June 6, 2000**	**705/3**
5,451,757	**September 19, 1995**	**340/5.4**
5,594,806	**June 20, 1994**	**382/115**

SPECIFICATIONS

ATM Second Personal Identification Number Emergency Response System

The Automatic Teller Machine Identification Number Emergency Response System gives each bank customer the option of holding an additional personal identification

numbers (P.I.N.) that will be used under hostile situations whereby customer is coerced into requesting money from a financial institution for a person, groups, or organizations under threat of life or limb. Any customer may go to their financial institution and request the option of having an additional personal identification number to use on their ATM or credit-card financial data to use only upon emergency situations. They will then key-in a second personal identification number that is separate and distinct from their first personal identification number. This additional personal identification number will be stored within the bank's central computers and shall be activated whenever customer types in their second P.I.N. number from within a bank branch, automatic teller machine, and/or telephone transaction with customer service representatives. When customer types in their second P.I.N. (hereafter known as the "emergency P.I.N. code") number, the A.T.M. machine will activate its communication systems (including, but not limited to modems, high speed internet connection, satellite, videophone) that will alert (but is not limited to) private security agencies, as well as public police agencies, including local, state, and federal officers (including the Federal Bureau of Investigation) to assist the victim(s) by noting that a customer has requested funds from a financial institution and that they are in immediate distress, concern, alarm, fear, and are in danger of bodily injury, death or loss of property. Time and location will be immediately transcribed to all security-related agencies, including local, state, and federal police agencies, as well as private security firms. A.T.M. machines will keep a consistently open and secure line of communication between machine and security agencies for immediate response. A.T.M. machines will record the date and time of the emergency requested for investigation-related purposes. When an emergency P.I.N. code has been typed in, A.T.M. machines

will dispense cash, balance transfers, deposits, without any written, audible, or visual image, code, notice, of any kind whatsoever near the ATM, phone, or any other medium victim utilizes, indicating emergency P.I.N. code has been keyed in and activated.